The State of Texas

Elections Division
P.O. Box 12060
Austin, Texas 78711-2060
www.sos.texas.gov

Phone: 512-463-5650
Fax: 512-475-2811
Dial 7-1-1 For Relay Services
(800) 252-VOTE (8683)

Ruth R. Hughs
Secretary of State

REPORT OF REVIEW OF HART INTERCIVIC VERITY VOTING 2.4 SYSTEM

PRELIMINARY STATEMENT

On April 13-17, 2020, Hart InterCivic Inc. ("Hart" or the "Vendor") presented Verity Voting 2.4 for examination and certification. The examination was conducted at Hart's offices in Austin, Texas. Pursuant to Sections 122.035(a) and (b) of the Texas Election Code, the Secretary of State appointed the following examiners:

1. Mr. Tom Watson, an expert in electronic data communication systems;
2. Mr. Brian Mechler, an expert in electronic data communication systems;
3. Mr. Brandon Hurley, an expert in election law and procedure; and
4. Mr. Charles Pinney, an expert in election law and procedure.

Pursuant to Section 122.035(a), the Texas Attorney General appointed the following examiners:

1. Dr. Jim Sneeringer, an expert in electronic data communication systems; and
2. Ms. Lesley French, an employee of the Texas Attorney General.

At the time of the examination, the Office of the Secretary of State was closed to the public due to health and safety concerns relating to the novel coronavirus (COVID-19). As a result, the examination of the Verity Voting 2.4 system was conducted at Hart's offices and certain procedures were implemented for the examination. For example, the examination was held over the course of five days, with no more than two examiners attending in person each day (rather than a traditional two-day examination with all examiners present at once). The examiners who were not physically present in the exam room were able to participate remotely via live video conference that allowed them to view the other examiners' interactions with the equipment and ask questions to the in-person examiners and the vendor. Each examiner had the opportunity to examine the equipment in person for at least one day during the exam week.

The Secretary of State's office also instituted social distancing and protective gear guidelines based on recommendations from the Centers for Disease Control and Prevention in response to COVID-19. The equipment was secured during the week of the examination using serialized seals on the door of the exam room, and a constant livestream video feed of the exam room was accessible to the examiners at any time throughout the exam week.

On April 13 and 14, 2020, Mr. Pinney was present at Hart's offices to witness the installation of the Verity Voting 2.4 software and firmware that the Secretary of State's office received directly from

New Since the Last Exam (on Dec. 13, 2015)

- The "Invalid vDrive" bug (which was discovered in the last examination) has been fixed.
- The Verity Verify system now has a DRE (a *direct-recording electronic* voting machine), the Verity Touch and Touch with Access.
- The Verity Touch has support for provisional electronic voting.
- The new Verity Data provides a graphical user interface for creating and managing election definitions.
- There is full support for cumulative voting.
- Reporting has been improved.

Security

Image Verification. To verify that the Build, Central, Count, User Management, Election Management, and Desktop software we tested is exactly the same as that certified by the Election Assistance Commission (EAC), the Secretary of State obtained the software images directly from the EAC. The software was then decompressed, loaded, and configured by Hart personnel under the supervision of the technical examiners, thus maintaining the chain of custody. This software is normally delivered to customers on hard drives that are pre-installed in the machines.

There is also a procedure that allows the county to verify that the software has not been tampered with. This is done by creating a manifest containing hashes of the files that the system comprises. The hashes are then compared with those on a manifest downloaded from the National Software Reference Library. If the hashes are the same, the files are also.

Verity Keys are USB drives used to control access to various parts of the Verity system. They contain no election data, and are used solely to restrict access to only those people who have the appropriate Verity Key. To gain access, the authorized person must insert the Verity Key and also enter a password. Verity Keys are not used in polling places, where only a user id and password are needed.

Election Setup

Election Definition. An election definition (containing races, candidates, etc.) is normally created with Verity Data. This is different from Verity 1, where the election definition was imported from a text file in XML format.

Verity Build. The election definition is then read by the Verity Build program, which allows the county to (a) proof the election, (b) proof the

System Summary

Overview. The Verity system comprises

(a) software components that run under Windows 7 on commercial-off-the-shelf (COTS) computer systems (1-7 above)
(b) devices for the polling place (8-13 above), and
(c) COTS components (such as computers, printers, and scanners).

Security

Chain of Custody. To verify that components we tested are the same as that certified by the Election Assistance Commission (EAC), the Secretary of State obtained the images directly from the EAC. Hart delivers its software components to customers on hard drives and its firmware components on memory cards known as CFAST. (CFAST is a newer version of Compact Flash memory, which is widely used in digital cameras. CFAST is short for Compact Fast, since CFAST is faster than Compact Flash.)

The hard drives and CFAST cards delivered by Hart require no software or firmware installation; once they have been inserted into the computer or other device, it is only necessary to switch on the power. Since the EAC sent the same kind of media Hart would give to customers, the examiners did not need to observe any installation procedures.

There is also a procedure that allows the customer to verify that the software has not been tampered with. This is done by creating a manifest containing hashes of the files that comprise the system. The hashes are compared with those on a manifest downloaded from the National Software Reference Library. If the hashes are the same, the files are also. We spot-checked the hash codes to verify again that we were examining the same products as the EAC.

Verity Keys are USB drives used to provide extra security (in addition to user IDs and passwords) to certain parts of the Verity system. They contain no election data and are used solely as tokens to restrict access to people who have the appropriate Verity Key and eight-digit passcode.

Verity Keys are not used in polling places, where only a six-digit numeric passcode is needed. Once again, the passcodes can be different for different operations, such as Open Polls, Close Polls, and spoil a ballot.

For security, Verity workstations used in the central-count office are run in *kiosk mode,* denying access to the operating system to anyone who does not have a special passcode available only from Hart support and valid for only one day.

Hart's complex ballot security system can be daunting, but it seems to be a robust system for guarding against unauthorized access. Nevertheless, there is some risk because the passcodes are the same throughout an election for all voting stations and other precinct devices.

Election Setup

The Hart Verity workstation software (Verity Data, Verity Build, etc.) can (a) create an election definition (containing races, candidates, ballot styles, etc.), (b) proof the election, (c) print ballots or create PDF files to send to a printer, (d) create Verity Keys, and (e) create *vDrives*, which convey election information to the voting devices and scanners.

vDrives are USB drives that are easily distinguishable from Verity Keys by shape and color. All vDrives contain the entire election definition and any vDrive for the election can be used to convey the election definition to any Verity device. For example, vDrives are used in polling places to initialize devices such as the Verity Touch, Verity Scan, and Verity Touch Writer Duo. vDrives for a given election all contain exactly the same data at first, for ease of creation and handling, but once a vDrive is used to initialize a device for the election, a unique ID is written on the vDrive, so every use of that vDrive can be traced in the audit logs.

When voting is over, the vDrives convey cast-vote records and logs to the counting location while the duplicate copy on the CFAST remains in the machine. All results are in clear text, but digitally signed so that their authenticity can be verified. Results are stored on vDrives in random order, to protect voter privacy. Should a vDrive have an invalid signature (or a signature from a different election), it will not be accepted.

Voting

Voting may be done (a) by hand-marking a paper ballot, (b) by voting on a Verity Touch, a direct-recording electronic (DRE) voting station, which records votes directly on both its vDrive and CFAST, or (c) by using either the Verity Touch Writer or the Verity Touch Writer Duo. The last two allow the voter to make selections on a touch screen and then print a marked ballot with those selections; they do not record the votes, except (of course) on the marked ballots that they print. The marked ballot from the Touch Writer looks like a traditional hand-marked ballot, while the ballot created by the Touch Writer Duo (called a PVR, for printed vote record) is printed in plain text that can be directly read by optical character recognition, with a hash in a QR code to detect any errors.

Voting can be done using the touch screen, but there is also support for disabled voters, such as audio, paddles, and sip-and-puff. Support for disabled voters was tested by the Secretary of State and is not covered by this report.

The voting devices seemed well-designed and easy to use, reducing the burden of both voters and poll workers. They present one race at a time to the voter, which in my opinion is the best method. I looked at the messages they presented in several situations (e.g. a ballot jam) and found them very understandable. I also spot-checked the Hart documentation for administrators and poll workers and found it understandable as well. It is still a formidable task to run an election, but good documentation and clear messages ease the burden significantly.

The Touch Writer does have the disadvantage that each voter must be authorized by a poll worker who physically walks to the Touch Writer, enters a password to gain access, and then selects the voter's precinct. In my opinion, this procedure is awkward and requires a lot of poll-worker time. However, a Touch Writer in every polling location would provide access to disabled voters.

The Touch Writer Duo does not have this disadvantage, because each voter is given a five-digit access code that controls ballot selection. Since voters on the Duo are also given a piece of thermal paper to record their choices, there is a small inconvenience, because they must enter their access code while holding both the blank "ballot" and the slip of paper containing the access code.

The Verity Controller controls voting at a group of Verity Touch or Touch Writer Duo stations. It issues the five-digit access codes that a voter must enter to begin voting.

Hart also offers Verity Scan, which can scan ballots in the polling place and store cast-vote records for later tabulation.

Tabulation, Reporting, and other Central Activities

Verity Central reads vDrives with results from the polling places and does ballot scanning, produces reports, and provides audit data. It can resolve issues and process write-ins and provisional votes, both for ballots it scanned and for those scanned in the precinct and then transported on a vDrive. Verity Central does not tabulate votes.

Verity Count tabulates the votes (stored in cast-vote records that came from a vDrive) and produces reports. It can also resolve issues and process write-ins.

Concerns

The Hart passcodes are the same for all voting stations and other precinct devices throughout the entire election. Since the same set of passcodes must be given to many people (at least one person at every voting location), it is imperative not to distribute the passcodes until just before the election.

The Hart devices share many common components, which is commendable. However, if Hart chooses to upgrade older customer devices to the newer ones, it should be done in such a way that the result is completely equivalent to the devices that have been certified.

Conclusion

I believe the Hart Verity system is one of the best we have examined. I am pleased that Hart has addressed several problems raised in previous exams.

I recommend certification of this system.

System Summary

Overview. The Verity system comprises

(a) software components that run under Windows 7 on commercial-off-the-shelf (COTS) computer systems (1-7 above)
(b) devices for the polling place (8-13 above), and
(c) COTS components (such as computers, printers, and scanners).

Security

Chain of Custody. To verify that components we tested are the same as that certified by the Election Assistance Commission (EAC), the Secretary of State obtained the images directly from the EAC. Hart delivers its software components to customers on hard drives and its firmware components on memory cards known as CFAST. (CFAST is a newer version of Compact Flash memory, which is widely used in digital cameras. CFAST is short for Compact Fast, since CFAST is faster than Compact Flash.)

The hard drives and CFAST cards delivered by Hart require no software or firmware installation; once they have been inserted into the computer or other device, it is only necessary to switch on the power. Since the EAC sent the same kind of media Hart would give to customers, the examiners did not need to observe any detailed installation procedures.

There is also a procedure that allows the customer to verify that the software has not been tampered with. This is done by creating a manifest containing hashes of the files that the system comprises. The hashes are compared with those on a manifest downloaded from the National Software Reference Library. If the hashes are the same, the files are also. I spot-checked the hash codes to verify again that we were examining the same products as the EAC; another examiner did a more comprehensive check.

Verity Keys are USB drives used to provide extra security (in addition to user IDs and passwords) to certain parts of the Verity system. They contain no election data and are used solely as tokens to allow access only to people who have the appropriate Verity Key and passcode.

Verity Keys are not used in polling places, where only a six-digit numeric passcode is needed. The passcodes can be different for different operations, such as Open Polls, Close Polls, and spoil a ballot.

There is some security risk in the polling places because the passcodes are the same throughout an election across all precincts for all voting stations and other precinct devices.

Concerns

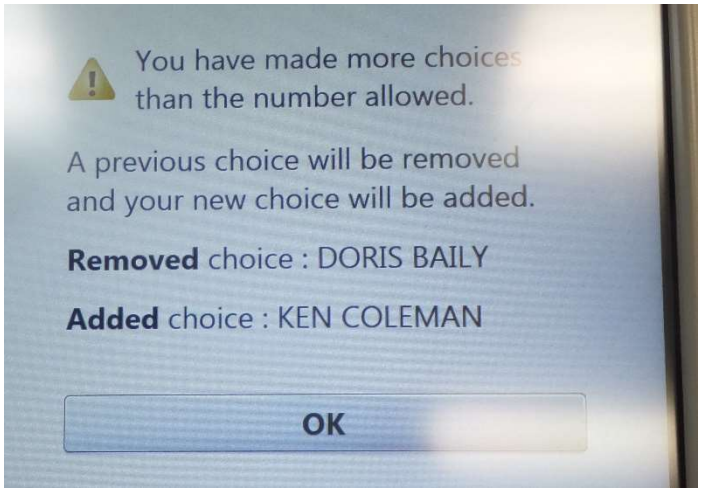
1. **Hash Code Verification.** There are several problems with the hash-code verification process.

    a. The names of the files to be verified using hash codes is read from a manifest file, which creates a risk if the manifest is not faithfully updated. It would be easy to overlook maintenance of the manifest; for example, some file lists in the Knowledge Base are out of date. Of course, not all files can be hashed and matched, because some are changed dynamically. However, it would be much better to maintain a list of the files ***not*** to be hashed. All DLL and EXE files should always be hashed, because they are never dynamic.

    b. For the Verity Controller, Touch, and Touch with Access, obtaining the hashes requires holding down a blue button for quite a long time. This is not intuitive, and its awkwardness creates a strong temptation to skip this important step.

    c. Hart recommends that the hashes be compared visually, which is difficult and error prone. As above, there is a temptation to skip this step. They should be automatically compared, although the individual hashes should be preserved for auditing.

2. **Multi-select Overvotes.** This affects all the Touch devices. Consider a race where one can vote for multiple candidates – say the voter can choose three of seven. If the voter has selected three candidates and tries to select a fourth, the TouchWriter will automatically deselect the first candidate selected, and give a message like the one in the photo to the right.


You have made more choices than the number allowed.
A previous choice will be removed and your new choice will be added.
Removed choice : DORIS BAILY
Added choice : KEN COLEMAN
OK

    Although the candidate who was deselected is unlikely to be the one the voter would have deselected, the voter can fix the problem. In the example, KEN COLEMAN is most likely the voter's last (fourth) choice, simply because the voter selected him last. In this case the voter can, after clearing the error message, deselect KEN COLEMAN and reselect DORIS BAILY. Note that it's not a good idea to simply clear the message and select DORIS BAILY, because the device might again choose the wrong candidate to deselect.

    I believe this is confusing, but acceptable because the voter can